Journal of Technology Research (JTR)
Volume 1, Issue 1, (2023), pp 083-093, ISSN 3005-639X

A Comparison of Data Hiding in Digital Colour Images Using the Improved Least Significant Bit Algorithm Based on the Three Color Channels with (2:2:4) and (2:3:3) Arrangements

Umm Al-Saad M. Al-Emilis[1]*, Issa A. Zwaid[1], Mohammed H. Abu Azzoum[1]

[1]The College of Industrial Technology, Misurata, Libya.

*Corresponding author email: omu_alam2001@yahoo.com

Received: 18-08-2023 | Accepted: 14-10-2023 | Available online: 15-12-2023 | DOI:10.26629/jtr.2023.07

ABSTRACT

The study aimed to introduce the concept of steganography, which is the science of concealing secret information within other media such as text, video, audio, or images. In image steganography, the digital image serves as a cover image in which the secret message is hidden, and the resulting image after embedding is known as the stego image. The work relied on the Improved Least Significant Bit (Improved LSB) technique by embedding data inside an RGB colour image in a way that preserves image quality while providing larger storage capacity for hidden information. The hiding process was implemented using the same algorithm in two modes: (2:2:4) and (2:3:3). In the first mode, 2 bits of secret data were hidden in the least significant part of the red channel (R), 2 bits in the green channel (G), and 4 bits in the blue channel (B). In the second mode, 2 bits were hidden in the red channel, while 3 bits were hidden in each of the green and blue channels. This algorithm is based on color theory, which states that the human eye is more sensitive to red and green than to blue. The results confirmed successful data hiding in both cases without noticeable distortion or visible artifacts, and the hidden data was retrieved with no loss, without requiring the original image or a location map. The implementation was carried out in MATLAB, where a program was designed for data embedding and extraction. Results of both methods were compared by evaluating image quality using Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), and Bit Error Rate (BER). Additionally, histograms were generated to illustrate color distribution differences between the original and stego images.

Keywords: Steganography, Cover Image, Secret message, Improved LSB, PSNR, MSE, BER.

مقارنة لعملية إخفاء البيانات داخل الصورة الرقمية الملونة باستخدام خوارزمية البت الأقل أهمية المطورة استنادا على قنوات الألوان الثلاثة على الترتيب (2:2:4) و(2:3:3)

ام السعد الاميلس[1]، عيسى عبد السلام زويد[1]، محمد حسين أبو عزوم[1]

[1] كلية التقنية الصناعة، مصراتة، ليبيا.

ملخـــــص البحـــــث

هدفت الدراسة الي التعريف بمفهوم إخفاء البيانات (Steganography) وهو علم إخفاء المعلومات السرية في أحد المصادر الأخرى مثل نص، فيديو، صوت، صورة ... إلخ. وفي علم الإخفاء الصوري (Image Steganography) تستخدم الصورة الرقمية كغطاء (Cover Image) حيث يتم فيها إخفاء الرسالة السرية (Secret message)، وتعرف الصورة الناتجة بعد

عملية الإخفاء باسم (Stego Image) . اعتمد العمل على تقنية البت الأقل أهمية المحسنة (Improved LSB) وذلك بتضمين معلومات داخل الصورة الملونة **RGB** بطريقة لا تؤثر علي جودة الصورة بعد الإخفاء مع توفير مساحة أكبر لإخفاء البيانات السرية. تتم عملية الإخفاء باستخدام نفس الخوارزمية ولكن بطريقتين الطريقة الاولي على الترتيب (2:2:4) والثانية على الترتيب (2:3:3) حيث تم بالترتيب الأول خزن2 بت من البيانات السرية في الجزء الأقل أهمية من حزمة اللون الأحمر **R** (البايت الأعلى أهمية) ،2 بت من البيانات السرية في الجزء الأقل أهمية من حزمة اللون الأخضر **G**، وأخيرا4 بت من البيانات السرية في الجزء الأقل أهمية من حزمة اللون الأزرق B. اما بالترتيب الثاني فتم إخفاء 3 بت في كل من قناة من قنوات اللون الأخضر والأزرق أما قناة اللون الأحمر فتم إخفاء 2 بت. هذه الخوارزمية تأتي اعتمادا على نظرية الالوان Color **Theory**التي تنص على أن العين البشرية أكثر تحسسا للونين الأحمر والأخضر مقارنة باللون الأزرق، حيث نجحت هذه الخوارزمية في الحالتين في إخفاء البيانات دون حدوث حالة تشوه للصورة الأصلية، أو إمكانية ملاحظة التغيرات الحاصلة فيها جراء عملية الإخفاء، وتم استرجاع تلك البيانات بسهولة دون فقدان لأي من مكوناتها، فضلا عن أن عملية الاسترجاع هذه تتم دون الاستعانة بالصورة الأصلية أو الحاجة لإنشاء جدول يبين مواقع الإخفاء. في هذا العمل تم الاعتماد على بيئة MATLAB في تصميم برنامج لإخفاء واستخلاص البيانات ومن ثم مقارنة النتائج في الحالتين بقياس جودة الصورة من خلال استخدام مقياس نسبة الإشارة إلى الضوضاء (PSNR)ومقياس مربع الخطأ (MSE)وكذلك مقياس معدل الخطأ في البتات (BER)، كما تم إظهار هيستوجرام الصورة والذي يبين الفرق في توزيع ألوان الصورة الاصلية والصورة الناتج.

الكلمات الدالة: اخفاء البيانات، صوره الغطاء، الرسالة السرية، تقنيه البث الاقل اهميه المحسنة، نسبة الإشارة إلى الضوضاء (PSNR)، ومقياس مربع الخطأ (MSE)، مقياس معدل الخطأ في البتات (BER).

1. المقدمة

في الاتصالات الرقمية بات من السهل اعتراض المعلومات المرسلة عبر شبكات الاتصال المختلفة أو الدخول الي الحاسبات سواء أكانت مرتبطة أو مستقلة عن الشبكة بقصد الاطلاع على محتوياتها أو سرقة معلوماتها أو العبث بها، وفي ضوء ذلك يتوجب تأمين الحماية والموثوقية والمصداقية للمعلومات والمحافظة عليها فظهرت وسائل حماية متنوعة مثل وضع كلمات سرية، أو استخدام التشفير (Cryptography) وكذلك تقنيات إخفاء أو تغطية البيانات(Steganography) ، وتتلخص عملية التشفير بتحويل الرسائل والبيانات السرية إلى صيغة لا يمكن قراءتها وذلك باستخدام مفتاح سري (Secret Key) ويتم استرجاعها باستخدام ذلك المفتاح [1].

1.1 مشكلة البحث

تكمن مشكلة البحث الأساسية في أن حماية البيانات عن طريق التشفير قد يجذب انتباه البعض لمهاجمة البيانات المشفرة (Encrypted Data) كما أن شكل الرسالة والبيانات الناتجة بعد عملية التشفير يثير الشك لظهور محتواها بشكل غير مرتب وظهور ألفاظ من غير اللغة المستخدمة مما يلفت انتباه المتطفلين أو قراصنة المعلومات إلى العبث بالرسالة إن لم يتمكنوا من فك الشفرة.

في المقابل توجد طريقة أخرى لإخفاء المعلومات وهي بأن نقوم بتضمينها داخل وسيط ما وتحت غطاء معين بحيث لا تظهر هذه الرسالة لمن يستعرض الوسيط الأساسي سواءً كان (صورة أو صوت أو فيديو) لأنها مخفية تمامًا داخله.

2.1 منهجية البحث

لكي تتم عملية الإخفاء يتم أولا تحويل البيانات السرية إلى سلسلة من البتات ومن ثم إخفائها في كل حزم الصورة اللونية بطريقتين الاولي علي

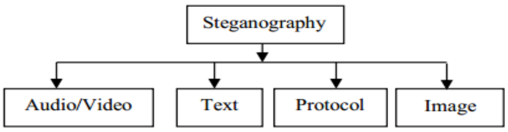
الترتيب (2:2:4) وذلك بتوزيعها كالاتي 2 بت في كل من حزم الالوان الأحمر R والأخضر G وذلك في الجزء الأقل أهمية من كل حزمة أو قناة لونية، و4 بت في الجزء الأقل أهمية لقناة اللون الأزرق B، أما الترتيب الثاني وهو (2:3:3) فيتم بإخفاء 2 بت بالجزء الأقل أهمية لحزمة اللون الأحمر، و3 بت بالجزء الأقل أهمية لكل من حزمة اللون الأخضر والازرق علي التوالي، وفي هذه لخوارزمية يمكن إخفاء كمية أكبر من البيانات حيث أن التلاعب بقيم البتات الأقل أهمية لا يؤثر على جودة الصورة أو قيمة اللون في كل قناة مما يجعل من الصعب على العين البشرية ملاحظة التغيير في الصورة الناتجة بعد الإخفاء.

3.1 أهداف البحث

الهدف الأساسي في أي عملية إخفاء هو الحفاظ على جودة الغطاء سواء كان صورة أو فيديو أو صوت مع إخفاء أكبر قدر من البيانات السرية، وفي هذا البحث تم إنشاء تطبيق يقوم بإخفاء البيانات واسترجاعها باستخدام خوارزمية البت الأقل أهمية المحسنة Improved LSB والتي من خلالها يتم إخفاء 8 بت في كل بكسل من بكسلات الصورة بدلا من إخفاء 3 بتات كما في خوارزمية LSB الأساسية.

2.تصنيفات الإخفاء وفقا لنوع الناقل

الناقل هو ملف البيانات الذي يتم فيه إخفاء البيانات السرية وذلك من خلال إجراء التعديلات عليه مثل ملفات الصور والمستندات وملفات الفيديو والملفات الصوتية والبروتوكول ويجب على الناقل أن يعمل بنفس طريقة الناقل الأصلي غير المعدل، وأن يظهر بشكل طبيعي لأي شخص يقوم بفحصه، يوضح الشكل (1) تصنيفات الإخفاء وفقا لنوع الناقل[3].



شكل1: تصنيفات الإخفاء وفقا لنوع الناقل.

1.2 الإخفاء بالنص Text Steganography

يمكن استخدام المستندات النصية لإخفاء المعلومات عن طريق إضافة مسافات بيضاء في نهاية أسطر المستند. وهذا النوع من الإخفاء فعال لأن الفضاء الأبيض يحدث بشكل طبيعي وغير مرئي للعين البشرية على الإطلاق وذلك في معظم برامج تحرير النصوص، وعند استخدام هذه التقنية فلا توجد طريقة للاشتباه في وجود أي بيانات مخفية[4].

2.2 الإخفاء بالصورة Image Steganography

يعد هذا النوع من الإخفاء من أكثر الأنواع شيوعاً في الاستخدام لما تتميز به الصور من صفات تجعلها الوسط المثالي للإخفاء، ويتم تطبيق هذه النوع من الإخفاء باستخدام العديد من الطرق منها الإخفاء باستخدام التحويل الزاوي المتقطع DCT، والإخفاء باستخدام التحويل الموجي DWT، وكذلك الإخفاء باستخدام الإدخال في البت الأقل أهميةLSB وهي أكثر الطرق شيوعاً [4].

3.2 الإخفاء بالصوت Audio Steganography

هناك العديد من التقنيات المستخدمة في إخفاء المعلومات داخل الملف الصوتي؛ التقنية المستخدمة عادة في إخفاء المعلومات داخل الملفات الصوتية هي تشفير بت منخفض يشبه LSB في ملفات الصور، ولكن باستخدام ترميز بت منخفض، وتعد هذه الطريقة محفوفة بالمخاطر لأنه عادة ما تكون ملحوظة للأذن البشرية. هناك طريقة أخرى تستخدم لإخفاء المعلومات داخل ملف صوتي وهي (Spread Spectrum)، وتعمل بإضافة ضوضاء عشوائية للإشارة، وتنتشر المعلومات عبر طيف التردد للملف الصوتي. طريقة أخرى لإخفاء المعلومات داخل ملف صوتي هي إخفاء بيانات (Echo) وتعمل هذه

الطريقة على إخفاء المعلومات ببساطة عن طريق إضافة صوت إضافي إلى صدى داخل الملف الصوتي[5] .

4.2 الإخفاء بالفيديو Video Steganography

عادة يتم إخفاء المعلومات داخل الفيديو باستخدام طريقةDCT، التي تعمل من خلال إجراء تغيير على كل صورة من صور الفيديو وذلك بتغيير القيم بأجزاء معينة من الصورة، لذلك لا تلاحظها العين البشرية، وإخفاء المعلومات في مقاطع الفيديو مشابهة لتلك الموجودة في الصور، بحيث يكون جزء من المعلومات مخفيا في كل إطار من الفيديو[6] .

5.2الإخفاء بالبروتوكولProtocolSteganography

يشير مصطلح " الإخفاء في البروتوكول " إلى تقنية تضمين المعلومات داخل الرسائل وبروتوكولات التحكم في الشبكة المستخدمة[7] .

3. مقاييس الأداء

يعتبر استخدام مقاييس أو معايير الأداء في تطبيقات تحسين الصور الرقمية له أهمية كبيرة في معرفة كفاءة التحسين الحاصلة لها، من ضمن هذه المقاييس مقياس نسبة الإشارة إلى الضوضاء (PSNR) Peak Signal-to-Noise Ratio، مقياس مربع الخطأ (MSE) Mean Square Error، مقياس معدل الخطأ في البتات Bit Error Rate(BER) وكذلك مقارنة هيستوجرام الصورة الأصلية والناتجة (Histogram) بعد عملية الإخفاء [8].

1.3 مقياس نسبة الإشارة إلى الضوضاء PSNR

يتم تطبيق هذا المصطلح على الصور كمقياس للجودة، وهو يشير الي نسبة الإشارة إلى الضوضاء حيث يعبر عن النسبة بين القيمة القصوى الممكنة للإشارة وقوة الضوضاء المشوهة التي تؤثر على جودة تمثيلها ويتم التعبير عن (PSNR) عادةً من حيث مقياس ديسيبل لوغاريتمي (dB) decibel كما في المعادلة:

$$(1)\ PSNR = 10\log_{10}\left(\frac{I_{max}^2}{MSE}\right) dB$$

حيث:

I_{max} : هي القيمة القصوى للإشارة الموجودة في الصورة الأصلية.

MSE: هومتوسط الخطأ التربيعي بين الصورة الاصلية أو صورة الغطاء cover image وبين الصورة الناتجة بعد عملية الإخفاء Stego image [9].

2.3 مقياس مربع الخطأ MSE

كما ذكر سابقا فان حساب قيمة نسبة الإشارة إلى الضوضاء (PSNR)يتطلب قياس مربع الخطأ(MSE) ويكون للصورة الرمادية حسب المعادلة التالية:

$$MSE = \frac{1}{M \times N}\sum_0^{M-1}\sum_0^{N-1}(CI(i,j) - SI(i,j))^2 \quad (2)$$

حيث:

N ,M عدد الصفوف والأعمدة للصورة الغطاء والصورة الناتجة.

(i, j) :CI هي قيمة البيكسل في الصورة الغطاء cover image (قبل الإخفاء) عند النقطة (i, j).

(i, j) :SI هي قيمة البيكسل في الصورة الناتجة Stego image عندالنقطة (i, j).

أما بالنسبة للصور الملونة، يتم حساب (MSE) بطريقتين الأولى بتحويل الصورة الملونة الى رمادية عبر استدعاء الدالة rgb2gray() ومن ثم استخدام القانون السابق، أو بحساب (MSE) على كل قيم البيكسل لكل قناة لونية على حدة ويتم حساب متوسطها بعدد قنوات الصورة الملونة والتي تحتوي على ثلاث قيم RGB لكل بكسل حسب المعادلة التالية:

$$(3)\quad MSE = \frac{1}{C.M.N}\sum(i_1 - i_2)^2$$

حيث:

i_2: i_1, قيمة البيكسل للصورتين الغطاء CoverImage والناتجة Stego Image

C: عدد قنوات الالوان [6].

3.3 مقياس معدل الخطأ في البتات BER

معدل الخطأ في البتات هو عدد أخطاء البتات لكل وحدة زمنية. وتقاس نسبة الخطأ البتات بعدد

أخطاء مقسوماً على العدد الإجمالي للبتات المنقولة خلال فترة زمنية معينة، وهي مقياس بدون وحدة.

في الإرسال الرقمي يكون عدد أخطاء البتات هو عدد البتات المستقبلة لتدفق البيانات عبر قناة اتصال تم تغييرها بسبب الضوضاء أو التداخل أو التشوه أو أخطاء التزامن في البتات، يتم حساب معدل الخطأ حسب المعادلة التالية:

$$(4)\ BER = \frac{1}{2} erfc\left(\sqrt{E_b/N_o}\right)$$

حيث :

E_b: عدد البتات الخاطئة

N_o : عدد البتات الكلي

كمثال، افترض تسلسل البتات المنقولة كالتالي:

1 1 0 1 0 0 0 1 1 0

وتسلسل البتات التي تم استقبالها كالتالي:

1 0 0 1 0 1 0 1 0 0

في هذه الحالة يكون عدد أخطاء البتات هو 3 بتات غير صحيحة مقسومة على 10 بتات تم نقلها، مما يؤدي إلى معدل BER يبلغ 0.3 أو 30%.[10]

4.3 مقياس الهيستوجرام Image Histogram

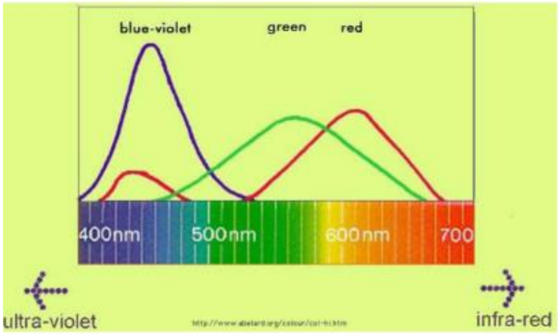
الهيستوجرام لأي صورة ملونة هو شكل بياني يوضح نسبة وجود الألوان فيها، بحيث يكون المحور الأفقي مبينا نسبة هذه الألوان بشكل متدرج بينما المحور العمودي هو القيمة الإجمالية لظهور ذلك اللون في الصورة، وبالنسبة لصور اللون الرمادي فيكون الهيستوجرام هو تمثيل بياني لمستويات الرمادي المختلفة في الصورة. وعلى هذا فلكل لون (أو قيمة رمادية) قيمة عددية تمثل في الشكل البياني وهي قيمة حدوثه في الصورة، وبمعالجة نسب الالوان والتدرجات يمكن عمل تأثيرات كثيرة على الصورة[11].

من المقاييس الأخرى التي كان لها دور في تحسين جودة الصورة طول النص وكذلك حجم صورة الغطاء حيث أن أفضل تأثير لإخفاء المعلومات هو عندما يكون حجم الصورة كبير، ويكون عدد البتات المطلوب إخفاؤها أقل، وكما أن إخفاء المعلومات في كل صفوف الصورة أفضل من إخفاءها في صف واحد من الصورة، حيث أن تأثير إخفاء المعلومات في النطاقات الملونة غير متساوٍ.

4. نظرية الألوان Color theory

تفسر هذه النظرية كيفية إدراك العين البشرية للألوان، وكيفية دمجها سواءً كانت متشابهة أو مختلفة.

يشير مصطلح رؤية اللون (Color vision) الي قدرة العين علي تمييز الأجسام اعتمادا على أطوال موجات الضوء (wavelengths) المنعكس عليها، ويميز الجهاز العصبي اللون بمقارنة استجابات الأنواع المختلفة من الخلايا المخروطية في العين للضوء حيث تكون هذه الخلايا حساسة لأجزاء مختلفة من الطيف المرئي، يوضح الشكل (2) أن هناك درجة من التداخل بين استجابات الخلايا المخروطية، حيث يتراوح الطيف المرئي للبشر تقريبا من 380 إلى 740 نانومتر، في هذا النطاق يكون اللونان الأحمر والأخضر أكثر حساسية للعين البشرية مقارنة بالأزرق[12] .



شكل 2: التداخل في الاطوال الموجية للألوان.

تعتبر مجموعة الألوان الأساسية بأنها مجموعة الألوان التي يمكن دمجها للحصول على تشكيلةٍ واسعةٍ من الألوان الأخرى. لكن أشهرها هو RGB، الذي يعتمد على الألوان الأحمر والأخضر والأزرق، والتي تدمج للحصول على بقية الألوان المختلفة بتدرجاتها جميعًا، وهو النموذج اللوني

المستخدم بكثرةٍ في شاشات التلفاز والحواسيب وآلات التصوير وغيرها[11].

وبما أن نظرية الألوان تنص على أن العين البشرية أقل تحسسا للون الأزرق من اللونين الاخرين وهما الأحمر والأخضر، فقد تم في هذا البحث اختيار طريقة إخفاء البيانات في الصورة الملونة بناء على هذا الأساس.

5.الدراسات السابقة لخوارزمية البت الأقل أهمية LSB (Least Significant Bit)

أجريت العديد من الدراسات والأبحاث التي كانت تحاول تطوير وتحسين تقنية LSB تحت اسم Improved LSB ومن هذه الدراسات، الدراسة التي قدمها (A. A. JAWAD) حول إخفاء المعلومات متعدد المستويات في العام 2003 ف، حيث يتم في المستوى الأول وضع الرسالة النصية في صورة من الابيض والاسود، والمستوى الثاني يأخذ من خرج المستوى الأول كمدخل الى صورة RGB. وكانت نتيجة هذه الدراسة أن الإخفاء متعدد المستويات له فوائد محتملة، حيث أنه يؤدي الي تعزيز سرية المعلومات باستخدام مستويين من الإخفاء ولكن مع اضافة المزيد من التعقيد في عملية إخفاء المعلومات من خلال تطبيقه في مستويين [13].

في العام 2008ف قدمت دراسة من قبل B.B. (Indradip) & (G.S. ISouvik) حيث ادرجت فكرة المفتاح السري للمصادقة عند كلا الطرفين وذلك باستخدام الترميز عند كلا الطرفين من أجل تحقيق مستوى عال من الأمن، وبالتالي يتم تنفيذ العملية العكسية لاسترجاع المعلومات الأصلية. وقد اضاف هذا النموذج مستوي عال من السرية، حيث أن الغطاء لا يدعو للشك بوجود رسالة ما داخله لأنها تبدو مشابهة الي الكائن الأصلي سواء كان الكائن صورة أو صوت أو فيديو [14].

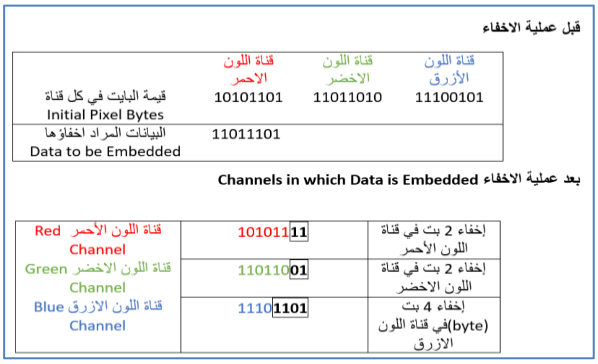
أما في العام 2009ف فقد قدمت دراسة من قبل R.R.) (Koppola وكان الهدف منها هو اقتراح تقنية جديدة مبنية على طريقة LSB لإخفاء كمية كبيرة من البيانات، وهذه التقنية تسمح بإخفاء صورة داخل صورة أخرى لها نفس الحجم وذلك بتقليل حجم الرسالة السرية قبل الإخفاء لإخفاء كمية أكبر من البيانات، ويتم إخفاء البيانات في مناطق من الصورة والتي لا تستطيع العين إدراك الاختلاف في الألوان فيها. من مساوئ هذه الدراسة أنها تعاني من فقدان البيانات عند الاسترجاع ولكنها تمتاز بجودة عالية بالإضافة الى إخفاء كمية كبيرة من البيانات [14].

في العام 2010ف قدمت دراسة (p. Halanka A.& Athawale) والتي اقترحت تحسين طريقة الخانة الثنائية الأقل أهمية لزيادة سعة التضمين والدقة، وهذه الطريقة يمكن تطبيقها على الصورة ذات الحجم 24 خانه ثنائية، وتم استخدام مفتاح سري طوله 8بت، وقبل أن تتم عملية التضمين تجري عملية (XOR) للمفتاح السري والخانات الثنائية في الرسالة وكل نقطة في الصورة وهذه الطريقة لها مميزات منها زيادة السعة لتضمين المعلومات مع جودة وأداء أفضل [14].

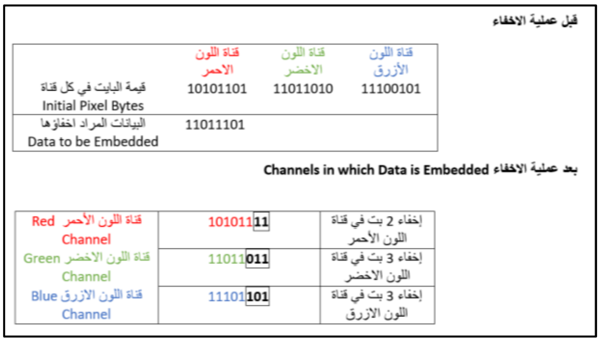
6. خوارزمية البت الأقل أهمية المحسنة على الترتيب (2:2:4) والترتيب (2:3:3) لكل قناة لونية RGB

في هذه الورقة تم العمل على خوارزمية البت الأقل أهمية المحسنة لإخفاء نص داخل صورة رقمية ملونة على الترتيب (2:2:4) مرة، والترتيب (2:3:3) مرة أخري وذلك لكل قناة لونية RGB حيث يمكن في الحالة الاولي أن تستبدل البت الثنائية الأقل أهمية الأولى والثانية في قناتي اللونيتين الأحمر والأخضر وكذلك البتات الثنائية الاربع من الجزء الأقل أهمية في قناة اللون الأزرق، أما الترتيب (2:3:3) فيتم فيه اخفاء 2 بت في قناة اللون الأحمر و3 بتات في كل قناة من قنوات اللون الأخضر والأزرق علي الترتيب مع بقاء العين البشرية غير قادرة على تمييز الفرق بين الصورتين فيما يلي مثال

لطريقة الإخفاء علي الترتيب (2:2:4)كما بالشكل (3) و الترتيب (2:3:3) كما بالشكل (4).



شكل3: طريقة LSB المحسنة على الترتيب (2:2:4).

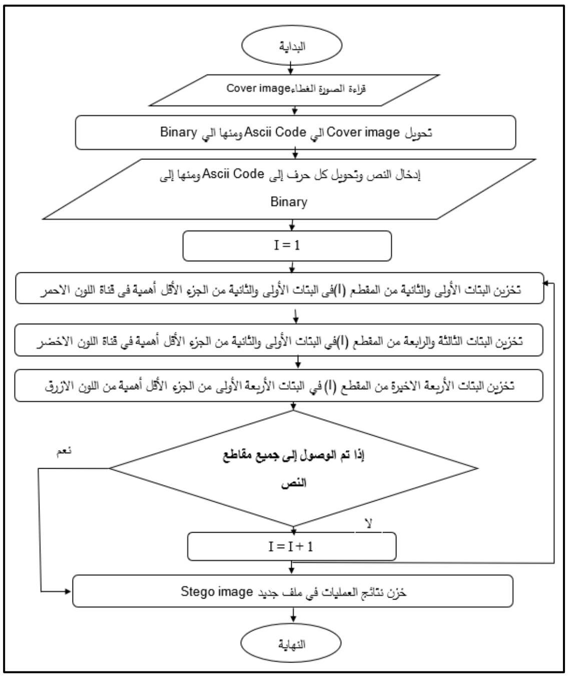


شكل4: طريقة LSB المحسنة على الترتيب (2:3:3).

1.6 خطوات عملية الإخفاء في خوارزمية البت الأقل أهمية المحسنة على الترتيب (2:2:4)

1. قراءة الصورة الرقمية الملونة cover image وتحديد أبعادها M, N وهو هي مناسبة بالحجم لإخفاء الرسالة السرية .
2. تحويل كل بكسل من الصورة الغطاء Cover Image إلي Code ASCII ومن ثم إلى الصيغة الثنائية binary.
3. إدخال النص المراد إخفاءه ومن ثم تحويل كل حرف الي CODE ASCII ومنه إلي الصيغة الثنائية binary.
4. يتم تخزين بتات النص في مصفوفه احادية (كأجزاء مكونة من 8 بت).
5. وضع قيمة عداد المقاطع I =1 والخاص بحساب عدد مقاطع بتات النص المراد إخفاءه.
6. تخزين البتات الأولي والثانية من المقطع I في البتات الأولى والثانية من الجزء الأقل أهمية في قناة اللون الأحمر.
7. تخزين البتات الثالثة والرابعة من المقطع I في البتات الأولى والثانية من الجزء الأقل أهمية في قناة اللون الأخضر.
8. تخزين البتات الأربعة الأخيرة من المقطع I في البتات الأربعة الأولى من الجزء الأقل أهمية في قناة اللون الأزرق.
9. إذا تم الوصول الي جميع المقاطع اذهب الي الخطوة (10) وإلا قم بزيادة العداد I = I +1 واذهب الي الخطوة (6).
10. خزن ناتج العمليات السابقة في ملف جديد بنفس نوع ملف الغطاء وهو ملف Stego image.

يوضح الشكل(5) المخطط الانسيابي لخطوات عملية الإخفاء.

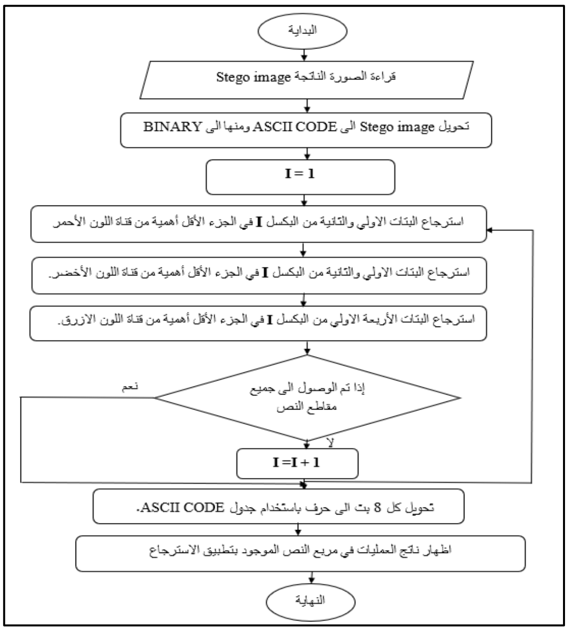


شكل 5: المخطط الانسيابي لخطوات عملية الإخفاء.

2.6 خطوات عملية الاسترجاع في خوارزمية البت الأقل أهمية المحسنة على الترتيب (2:2:4)

1. قراءة ملف الصورة الناتجة Stego image الذي يحتوي على البيانات المخفية بداخله.
2. تحويل كل بكسل من الصورة الي ASCIICode ومن ثم إلى الصيغة الثنائية binary.
3. وضع قيمة عداد المقاطع I =1 والخاص بحساب عدد مقاطع بتات النص المراد استرجاعه
4. استرجاع البتات الأولي والثانية من البكسل I في الجزء الأقل أهمية من قناة اللون الأحمر.
5. استرجاع البتات الأولي والثانية من البكسل I في الجزء الأقل أهمية من قناة اللون الأخضر.
6. استرجاع البتات الأربعة الأولي من البكسل I في الجزء الأقل أهمية من قناة اللون الأزرق.
7. إذا تم الوصول الي جميع بتات مقاطع النص المراد استرجاعه اذهب الي الخطوة (8) والا قم بزيادة العداد I = I +1 والذهاب الي الخطوة (4).
8. تحويل كل 8 بت الي حرف باستخدام جدول ASCII CODE.

يوضح الشكل(6) المخطط الانسيابي لخطوات عملية الاسترجاع.

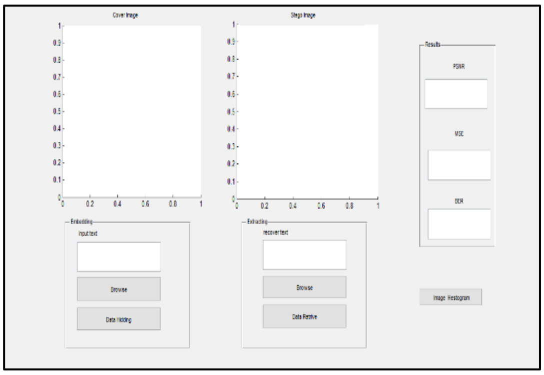


شكل6: المخطط الانسيابي لخطوات عملية الاسترجاع.

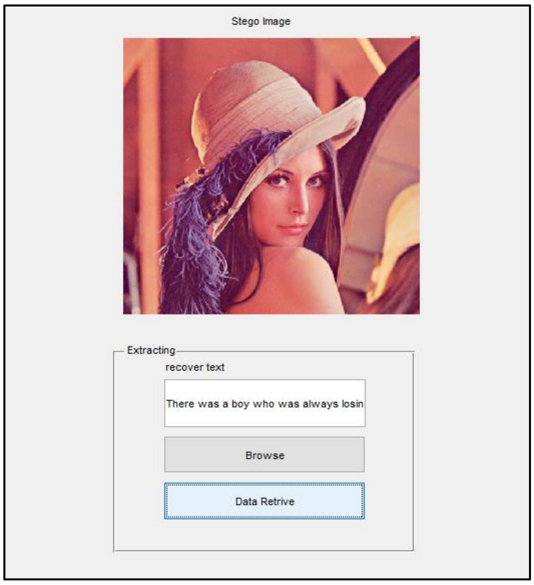
في الترتيب الثاني تم اتباع نفس الخطوات عندما كان ترتيب الاخفاء على الطريقة (2:2:4) ولكن مع اختلاف الترتيب ليكون على النحو التالي (2:3:3).

7. تصميم وتنفيذ البرنامج

تم في هذه المرحلة تصميم الواجهة الرئيسية للبرنامج، حيث تحتوي هده الواجهة على خيارات يتم فيهن إظهار الصور الاصلية cover image والصورة التي تم إخفاء النص داخلها Stego image، كما تحتوي على خيارات ترتيب إخفاء النص أو إظهار النص المخفي، كذلك تحتوي الشاشة على مجموعة من المقاييس التي يتم حسابها بالبرنامج بالإضافة الي زر يقوم بإظهار هيستوجرام الصورة قبل وبعد الإخفاء، كما هو موضح بالشكل (7). كما يظهر الشكل (8) خيار إخفاء النص داخل الصورة.

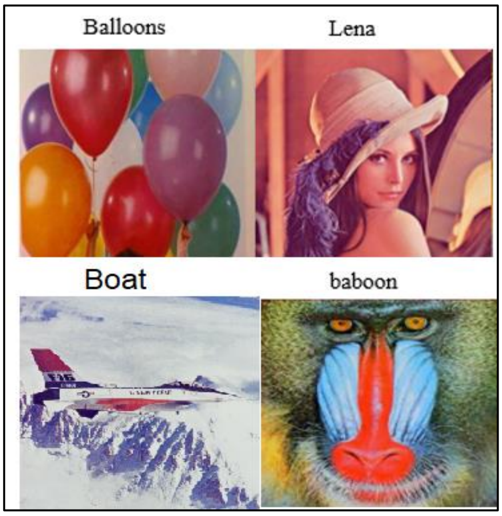


شكل7: الواجهة الرئيسية للبرنامج.



شكل8: واجهة إخفاء نص داخل صورة.

تـم فـي البرنـامج اسـتخدام عـدد مـن الصـور ذات الامتداد (JPG.) كما موضحة بالشكل (9).



شكل9: الصور المستخدمة كغطاء.

8.النتائج

تم اختبار الصـــور بمقاييس جودة الصـــورة وهي نســـبة الإشـارة الي الضـوضـاء (PSNR)، معدل الخطأ (MSE) وأخيرا معدل الخطأ في البتات (BER) ومقارنة النتائج في الحالتين كما بالجدول (1) والجدول (2).

جدول رقم (1): نتائج اختبار مقاييس الأداء عند الترتيب (2:2:4).

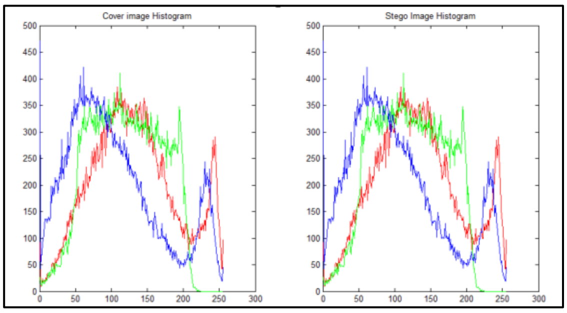
اسم الصورة	مقاييس الأداء		
	PSNR	MSE	BER
Baboon	54.83	0.16	0.050
Lena	61.92	0.17	0.049
Balloons	56.13	0.16	0.050
Boat	56.85	0.16	0.049

جدول رقم (2): نتائج اختبار مقاييس الأداء عند الترتيب (2:3:3).

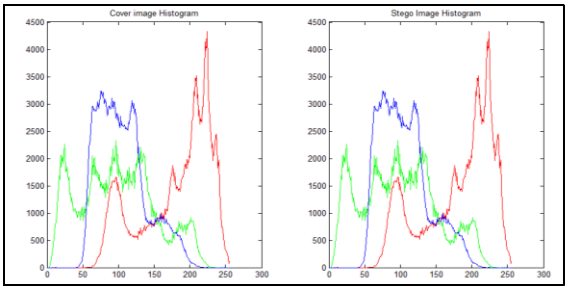
اسم الصورة	مقاييس الأداء		
	PSNR	**MSE**	**BER**
Baboon	53.99	0.17	0.050
Lena	61.32	0.18	0.048
Balloons	55.80	0.16	0.051
Boat	56.55	0.16	0.050

نســـتنتج من جداول النتائج الســـابقة ان الخوارزمية علي الترتيبين (2:2:4) و (2:3:3) قد أعطت نتائج متقاربة جدا في مقاييس الأداء مع وجود اختلاف بسـيط حيث تم الاخفاء بالجزء الأقل أهمية لقناة اللون الأزرق بفارق 4 بت عند اختيار الترتيب (2:2:4) بدلا من 3 بتات بالترتيب (2:3:3) وبالتالي تأتي جودة الصـــورة بالنســـبة للعين البشـــرية بعدم ملاحظة أي تأثير أو اختلاف في صورة الغلاف بالدرجة الأولي، بحيث يمكن أن تتم عملية الإخفاء دون ملاحظة وجود أي بيانـات داخلها، وذلك اعتمادا على نظرية الألوان color theory التي تنص على أن قدرة العين البشـــرية للتميز بين التدرجات الرقمية القريبة الضـــعيفة فضـــلا على قدرتها علي التمييز في التدرجات الغامقة، وحســـب نظام الرؤية البشـــرية HVS فإن العين البشـرية أقل تحسـسا للون الأزرق من اللونين الآخرين(الأحمر والأخضر).

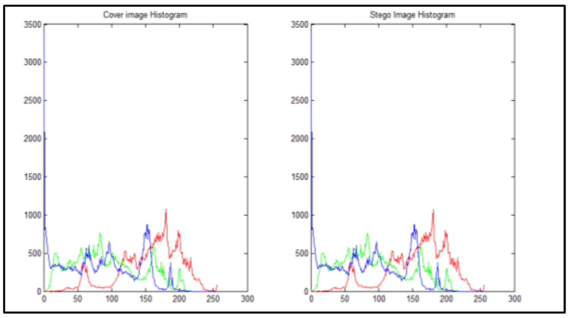
بالنسـبة لمخطـط الهيسـتوجرام فقد تم الحصـول علـى مخططـات الألـوان الموجـودة بكـل صـورة وذلـك قبـل وبعــد عمليــة الإخفــاء كمــا بالأشــكال (10) (11) (12)، والتــي توضــح أن توزيــع الألــوان كــان متطابقــا لكل صورة قبل وبعد التعديل عليها.



شكل10: هيستوجرام صورة baboon.



شكل11: هيستوجرام صورة Lena.



شكل12: هيستوجرام صورة Balloons.

9. الاستنتاجات

أ- أعطت الخوارزمية في الترتيبين نتائج جيدة من ناحية مقاييس الأداء وكذلك جودة الصورة، حيث أن مقياس (PSNR) أعطى قيم عالية والذي يوضح نسبة الإشارة إلى الضوضاء مما يعني أن الصورة الناتجة كانت قريبة من الصورة الأصلية.

ب- مقياس (MSE) أعطى قيم ضئيلة جدا في نسبة التغير بين الصورة الأصلية والناتجة.

ت- مقياس (BER) فقد أعطى أيضا قيم ضئيلة جدا في عدد أخطاء البتات.

ث- بالنسبة الي هيستوجرام الصور الأصلية والناتجة فقد أظهر توزيعا متقاربا في الألوان قبل وبعد عملية الإخفاء.

ج- عند استخدام صور عالية الجودة يمكن الحصول علي نتائج أفضل .

10. التوصيات

أ- يمكن استخدم ترتيب آخر للبيانات مثل .(1:3:4)

- قد يعطي استخدام صور بامتداد من نوع آخر كصورة غطاء نتائج مختلفة.

ت- يمكن إخفاء صورة داخل صورة أو صوت أو فيديو، كما يمكن إخفاء البيانات في غطاء أخر بدلا من الصورة مثل الصوت أو الفيديو.

ث- لزيادة لأمن والحماية بالإمكان تشفير البيانات قبل عملية الإخفاء.

11. الخاتمة:

تم في هذه الورقة العمل على إخفاء بيانات نصية في صورة رقمية ملونة باستخدام خوارزمية البت الأقل أهمية المحسنة (Improved LSB) وذلك على الترتيبين (2:2:4) و (2:3:3) بت في كل قناة لونية RGB، فقد تم بالترتيب الاول تجزئة البايت المراد اخفاؤه الي ثلاث أجزاء يحتوى الجزء الأول والثاني علي 2 بت وتم اخفاؤها في الجزء الأقل أهمية من بايت كل قناة من الألوان (الأحمر والأخضر) بينما تم إخفاء الأربع بتات الاخيرة في الجزء الأقل أهمية من بايت قناة اللون الأزرق، اما بالترتيب (2:3:3) فقد احتوى الجزء الأقل أهمية لقناة اللون (الأحمر) علي 2 بت، بينما احتوى الجزء الأقل أهمية للقنوات اللونية (الأخضر والأزرق) على 3 بتات لكل قناة، وقد كانت النتائج متقاربة الي حد ما مع وجود اختلاف بسيط جدا في قراءة المقاييس والذي يرجع الي اختلاف الترتيب . وقد تبين ان هذه النتائج تعطي إمكانية إخفاء كميات كبيرة من البيانات داخل الصورة بحيث لا يحدث تغير في الصورة من ناحية جودة الأداء.

المراجع:

[1] Wang Y, Tang M, Wang Z. High-capacity adaptive steganography based on LSB and Hamming code. *Optik*. 2020;213:164685.

[2] Devi M, Sharma N. Improved detection of least significant bit steganography algorithms in color and gray scale images. In: *Recent Advances in Engineering and Computational Sciences (RAECS)*. IEEE; 2014. p. 1-5.

[3] Hegde R, S J. Design and implementation of image steganography by using LSB replacement algorithm and pseudo random encoding technique. *Int J Recent Innov Trends Comput Commun*. 2015 Jul;3(7):4415-20.

[4] Koppola RR. A high-capacity data-hiding scheme in LSB-based image steganography [dissertation]. Akron: University of Akron; 2009.

[5] Kuo WC, Wang CC, Hou HC. Signed digit data hiding scheme. *Inf Process Lett*. 2015 Aug;5(2):15-26.

[6] Jarno M. LSB matching revisited. *IEEE Signal Process Lett*. 2006 May;13(5):285-7.

[7] Al-Bayati M, Al-Jarrah MM. The hiding of multimedia secret files in dual RGB cover images using LSB steganography techniques. *Comput Sci*. 2016.

[8] Rita C, Deepika B. An improved DCT based steganography technique. *Int J Comput Appl*. 2014 Sep;102(14):46-9.

[9] Al-Emilis UM, Al-Jaroushi FI. استخدام الصور الرقمية مقارنة بين طرق الإخفاء المعتمدة على قيم البكسل والبت الأقل أهمية. In: *Third International Conference on Technical Sciences (ICST2020)*; 2020 Nov 28-30; Tripoli, Libya.

[10] Kekre HB, Athawale A, Halarnkar PN. Increased capacity of information hiding in LSBs method for text and image. *Int J Electr Comput Syst Eng*. 2008;2(4).

[11] Pan HK, Tseng YC, Chen YY. A secure data hiding scheme for binary images. *IEEE Trans Commun*. 2002 Aug;50(8):1227-31.

[12] Alqadi Z, Zahran B, Jaber Q, Ayyoub B, Al-Azzeh J. Enhancing the capacity of LSB method by introducing LSB2Z method. *Int J Comput Sci Mob Comput*. 2019;8(3):76-90.

[13] Abelard.org. Colour vision and art. Available from: http://www.abelard.org/colour/col-hi.htm